

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-265217**
 (43)Date of publication of application : **28.09.2001**

(51)Int.Cl.

G09C 1/00
G06F 12/14

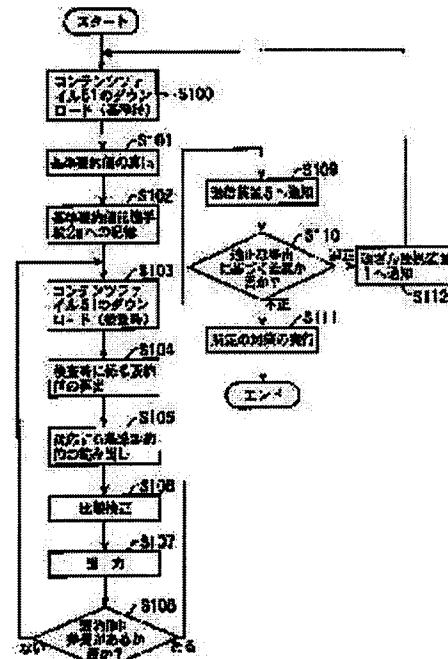
(21)Application number : **2000-076967**(22)Date of filing : **17.03.2000**(71)Applicant : **CTI CO LTD**(72)Inventor : **SUZUKI SHUNYO**
MURASE SHINJI
SUGIE OSAMU

(54) DEVICE AND METHOD FOR MONITORING ALTERATION OF DIGITAL CONTENTS, AND RECORDED MEDIUM THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To call attention to whether or not a change in digital contents is unauthorized, by speedily detecting the change in the digital contents and outputting the result for notification.

SOLUTION: A summed -up value calculating means for calculating a summed -up value of a content file related to digital contents to be monitored by a unidirectional function, is provided, a summed -up value at the reference time and that at the inspection time are compared with each other. Therefore, it is possible to detect at an early stage the fact of a change in the contents. By outputting the verification result of the comparison and notifying the information supplier of the digital contents to be monitored thereof, it is possible to call their attention to whether the change is unauthorized, and prevent the scale of damage from expanding. Moreover, since any change is being monitored by using a summed -up value by a unidirectional function, comparison verification can be performed speedily.



LEGAL STATUS

[Date of request for examination] **09.03.2007**

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-265217

(P2001-265217A)

(43)公開日 平成13年9月28日 (2001.9.28)

(51)Int.Cl.⁷

G 0 9 C 1/00

識別記号

6 4 0

F I

テ-ヤ-ト*(参考)

C 0 9 C 1/00

6 4 0 D 5 B 0 1 7

G 0 6 F 12/14

3 1 0

C 0 6 F 12/14

6 4 0 Z 5 J 1 0 4

3 1 0 Z 9 A 0 0 1

審査請求 未請求 請求項の数12 OL (全 9 頁)

(21)出願番号

特願2000-76967(P2000-76967)

(22)出願日

平成12年3月17日 (2000.3.17)

(71)出願人 599105850

株式会社シーティーアイ

愛知県名古屋市中村区名駅南一丁目27番2号

(72)発明者 鈴木 春洋

愛知県名古屋市中村区名駅南一丁目27番2号 株式会社シーティーアイ内

(72)発明者 村瀬 胜二

愛知県名古屋市中村区名駅南一丁目27番2号 株式会社シーティーアイ内

(74)代理人 100073139

弁理士 千田 稔 (外1名)

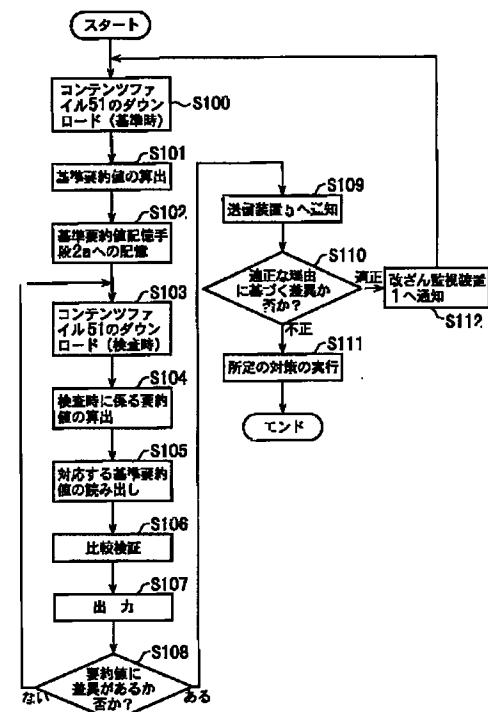
最終頁に続く

(54)【発明の名称】 デジタルコンテンツの改ざん監視装置、改ざん監視方法及び記録媒体

(57)【要約】

【課題】 デジタルコンテンツの内容変更を速やかに発見し、その結果を出力して知らせることで、不正な改ざんによるものか否かの注意を喚起する。

【解決手段】 監視対象となるデジタルコンテンツに係るコンテンツファイルの、一方向関数による要約値を算出する要約値算出手段を設定し、基準時に係る要約値と検査時に係る要約値とを比較する。従って、内容が変更された事実を早期に発見できる。比較検証結果を出力して監視対象となっているデジタルコンテンツの情報提供者に知らせることで、不正な改ざんによるものか否かの注意を喚起でき、被害規模の拡大を防ぐことができる。また、一方向関数による要約値を用いて監視しているため、比較検証を迅速に行うことができる。



【特許請求の範囲】

【請求項1】 ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視装置であつて、監視対象となるデジタルコンテンツに係るコンテンツファイルの、一方向関数による要約値を算出する要約値算出手段と、前記要約値算出手段により算出した前記デジタルコンテンツの基準時に係るコンテンツファイルの要約値が、基準要約値として記憶されている記憶手段と、前記要約値算出手段により算出した前記デジタルコンテンツの検査時に係るコンテンツファイルの要約値を、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証する比較検証手段と、前記比較検証手段による検証結果を出力する出力手段とを具備することを特徴とするデジタルコンテンツの改ざん監視装置。

【請求項2】 請求項1記載のデジタルコンテンツの改ざん監視装置であつて、前記送信装置がウェブサーバであり、前記デジタルコンテンツがウェブページであることを特徴とするデジタルコンテンツの改ざん監視装置。

【請求項3】 請求項1又は2記載のデジタルコンテンツの改ざん監視装置であつて、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とするデジタルコンテンツの改ざん監視装置。

【請求項4】 請求項1～3のいずれか1に記載のデジタルコンテンツの改ざん監視装置であつて、前記基準要約値を用いた電子署名が付加されて記憶されていることを特徴とするデジタルコンテンツの改ざん監視装置。

【請求項5】 監視対象となるデジタルコンテンツの基準時に係るコンテンツファイルの、一方向関数による要約値を算出し、記憶手段に基準要約値として記憶させるステップと、前記デジタルコンテンツの検査時に係るコンテンツファイルの、一方向関数による要約値を算出し、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証するステップと、

前記ステップによる検証結果を出力するステップとを具備し、ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体。

【請求項6】 請求項5記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であつて、前記送信装置がウェブサーバであり、前記デジタルコンテンツがウェブページであることを特徴とする記録媒体。

【請求項7】 請求項5又は6記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録

した記録媒体であつて、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とする記録媒体。

【請求項8】 請求項5～7のいずれか1に記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であつて、前記記憶手段に基準要約値を記憶させるステップにおいては、当該基準要約値の電子署名を作成し、当該電子署名を附加して記憶させるように設定されることを特徴とする記録媒体。

【請求項9】 ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視方法であつて、

監視対象となるデジタルコンテンツの基準時に係るコンテンツファイルの、一方向関数による要約値を算出し、コンピュータの記憶手段に基準要約値として記憶させる工程と、

前記デジタルコンテンツの検査時に係るコンテンツファイルの、一方向関数による要約値を算出し、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証する工程と、

前記ステップによる検証結果を出力する工程とを具備することを特徴とするデジタルコンテンツの改ざん監視方法。

【請求項10】 請求項9記載のデジタルコンテンツの改ざん監視方法であつて、前記送信装置がウェブサーバであり、前記デジタルコンテンツがウェブページであることを特徴とするデジタルコンテンツの改ざん監視方法。

【請求項11】 請求項9又は10記載のデジタルコンテンツの改ざん監視方法であつて、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とするデジタルコンテンツの改ざん監視方法。

【請求項12】 請求項9～11のいずれか1に記載のデジタルコンテンツの改ざん監視方法であつて、前記記憶手段に基準要約値を記憶させる工程においては、当該基準要約値の電子署名を作成し、当該電子署名を附加して記憶させるものであることを特徴とするデジタルコンテンツの改ざん監視方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、デジタルコンテンツの改ざん監視装置、監視方法及びデジタルコンテンツの改ざん監視をコンピュータに実行させるための記録媒体に関する。

【0002】

【従来の技術】 近年、コンピュータネットワークの急速な普及により、インターネットのウェブページなどの形式で、不特定多数を対象に公開されるデジタルコンテンツが多くなってきている。

【0003】

【発明が解決しようとする課題】しかしながら、同時にまた、例えば、WWW (World Wide Web) 上の送信サーバ(送信装置)への不正アクセスなどによって、ウェブページ(ホームページ)の内容が改ざんされる事故も増加している。

【0004】本発明は上記した点に鑑みなされたものであり、ウェブページのような不特定多数を対象に提供されるデジタルコンテンツの内容変更を速やかに発見し、その結果を出力して知らせることで、不正な改ざんによるものか否かの注意を喚起できるデジタルコンテンツの改ざん監視装置、監視方法及びデジタルコンテンツの改ざん監視をコンピュータに実行させるための記録媒体に関する。

【0005】

【課題を解決するための手段】上記課題を解決するため、請求項1記載の本発明のデジタルコンテンツの改ざん監視装置は、ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視装置であって、監視対象となるデジタルコンテンツに係るコンテンツファイルの、一方向関数による要約値を算出する要約値算出手段と、前記要約値算出手段により算出した前記デジタルコンテンツの改ざん監視装置に係るコンテンツファイルの要約値が、基準要約値として記憶されている記憶手段と、前記要約値算出手段により算出した前記デジタルコンテンツの改ざん監視装置に係るコンテンツファイルの要約値を、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証する比較検証手段と、前記比較検証手段による検証結果を出力する出力手段とを具備することを特徴とする。

【0006】請求項2記載の本発明のデジタルコンテンツの改ざん監視装置は、請求項1記載のデジタルコンテンツの改ざん監視装置であって、前記送信装置がウェブサーバであり、前記デジタルコンテンツがウェブページであることを特徴とする。

【0007】請求項3記載の本発明のデジタルコンテンツの改ざん監視装置は、請求項1又は2記載のデジタルコンテンツの改ざん監視装置であって、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とする。

【0008】請求項4記載の本発明のデジタルコンテンツの改ざん監視装置は、請求項1～3のいずれか1に記載のデジタルコンテンツの改ざん監視装置であって、前記基準要約値を用いた電子署名が付加されて記憶されていることを特徴とする。

【0009】請求項5記載の本発明の記録媒体は、デジタルコンテンツの改ざん監視装置は、監視対象となるデジタルコンテンツの基準時に係るコンテンツファイルの、一方向関数による要約値を算出し、記憶手段に基準要約値として記憶させるステップと、前記デジタルコン

テンツの検査時に係るコンテンツファイルの、一方向関数による要約値を算出し、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証するステップと、前記ステップによる検証結果を出力するステップとを具備し、ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録したことを特徴とする。

【0010】請求項6記載の本発明の記録媒体は、請求項5記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であって、前記送信装置がウェブサーバであり、前記デジタルコンテンツがウェブページであることを特徴とする。

【0011】請求項7記載の本発明の記録媒体は、請求項5又は6記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であって、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とする。

【0012】請求項8記載の本発明の記録媒体は、請求項5～7のいずれか1に記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であって、前記記憶手段に基準要約値を記憶させるステップにおいては、当該基準要約値の電子署名を作成し、当該電子署名を付加して記憶させるように設定されることを特徴とする。

【0013】請求項9記載の本発明のデジタルコンテンツの改ざん監視方法は、ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視方法であって、監視対象となるデジタルコンテンツの基準時に係るコンテンツファイルの、一方向関数による要約値を算出し、コンピュータの記憶手段に基準要約値として記憶させる工程と、前記デジタルコンテンツの改ざん監視装置に係るコンテンツファイルの、一方向関数による要約値を算出し、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証する工程と、前記ステップによる検証結果を出力する工程とを具備することを特徴とする。

【0014】請求項10記載の本発明のデジタルコンテンツの改ざん監視方法は、請求項9記載のデジタルコンテンツの改ざん監視方法であって、前記送信装置がウェブサーバであり、前記デジタルコンテンツがウェブページであることを特徴とする。

【0015】請求項11記載の本発明のデジタルコンテンツの改ざん監視方法は、請求項9又は10記載のデジタルコンテンツの改ざん監視方法であって、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とする。

【0016】請求項12記載の本発明のデジタルコン

ンツの改ざん監視方法は、請求項9～11のいずれか1に記載のデジタルコンテンツの改ざん監視方法であって、前記記憶手段に基準要約値を記憶させる工程においては、当該基準要約値の電子署名を作成し、当該電子署名を付加して記憶させるものであることを特徴とする。

【0017】

【発明の実施の形態】以下、本発明を図面に示した実施形態に基づいて更に詳しく説明する。図1は、本発明の一の実施形態にかかる改ざん監視装置1の構成図である。この図に示したように、この改ざん監視装置1はコンピュータから構成され、CPU、メモリやハードディスクドライブなどの記憶手段2を有すると共に、入出力制御部4を介して接続されたモニタ3などのハードウェアを有し、さらに所定のOSがインストールされている。また、本実施形態においてデジタルコンテンツの改ざん監視を行うための制御手段10として機能するプログラムが記憶手段2にインストールされる。

【0018】本実施形態の制御手段10であるプログラムは、一方向関数による要約値を算出する要約値算出手段11を備えている。要約値算出手段11は、監視対象となるデジタルコンテンツに係るコンテンツファイルを、一方向関数により要約する手段である。監視対象となるデジタルコンテンツは、複数の端末からアクセスされることによって、自動送信される形態で開示されているものであれば何であってもよく、例えば、ウェブサーバ(送信装置5)によって提供される任意のウェブページ(ホームページ)上の情報が挙げられる。特に、近年、第三者の不正アクセスによるウェブページ(ホームページ)の改ざんが頻出しているので、これを監視対象とすることにより本発明を有効に利用できる。もちろん、パソコン通信等によって提供されるデジタルコンテンツであってもよい。

【0019】また、このデジタルコンテンツの内容に制限はなく、テキストデータ、画像データ等の種々のデータであってよいが、例えば、日付やアクセスカウンタなどのように常に変化するデータを含めると、それらが変化するだけでも要約値が変化してしまうことから、このようなデータは監視対象となるデジタルコンテンツから除外しておくことが好ましい。

【0020】上記したデジタルコンテンツに係るコンテンツファイルの入手方法は任意であるが、監視対象とするウェブページの情報提供者(送信装置5の管理者ないしは運営者)と本実施形態の改ざん監視装置1の管理者ないしは運営者との間で契約が結ばれたならば、改ざん監視装置1から監視対象となるウェブページにインターネットを利用してアクセスし、当該監視装置1にコンテンツファイルをダウンロードすることにより入手したり、あるいは、コンテンツファイルを記録したCD-ROM、DVD、フレキシブルディスクなどの記録媒体を入手して改ざん監視装置1に記憶させることもできる。

また、送信装置5に記録されているコンテンツファイル51を専用回線などによって監視装置1に記憶させることもできる。

【0021】要約値を算出する具体的な手段としては、典型的には、ハッシュ関数を利用することが好ましい。ハッシュ関数とは、ファイルを一定の長さ(例えば、128ビット)のハッシュ値に圧縮する関数であり、変換された文字列から元の文字列を見つけだすことがほとんど不可能な強一方指向であると共に、元の文章が1ビットでも異なれば結果として得られるハッシュ値が大きく変わるという特徴をもっている。ハッシュ関数の種類は限定されるものではなく、例えば、MD-5、MASH、米国標準技術局のSHA-1などを用いることができる(図3参照)。

【0022】制御手段10であるプログラムは、また、上記要約値算出手段11によって、基準時に係るコンテンツファイル51のハッシュ値を算出して、さらにそれを基準要約値として記憶手段2の一部に形成した基準要約値記憶部2aに記憶させるステップを備えている。ここで、基準時とは、上記の例でいえば、監視対象となるウェブページの情報提供者との間で契約成立後に、初めてダウンロードする時、あるいは、当該情報提供者が記録媒体の形式でコンテンツファイル51を提供する場合における当該コンテンツファイル51の記録媒体への記録時などをいうが、不正な改ざん等がなされていない状態の比較基準となるコンテンツファイル51を特定した時点であればこれらに限定されるものではない。

【0023】また、デジタルコンテンツ(ウェブページ)の内容が適正に更新された場合には、更新されたコンテンツファイル51の要約値を基準とする必要があるため、その際には、更新されたコンテンツファイル51をダウンロードなどにより特定した時点が基準時となる。

【0024】また、制御手段10であるプログラムは、任意の検査タイミングで、例えば、数分おき、数時間おき、毎日所定時刻、数日おきなどのタイミングで、監視対象となっているウェブサーバにアクセスし、所定のデジタルコンテンツ(ウェブページ)のコンテンツファイル51を記憶手段2にダウンロードし、当該コンテンツファイル51の要約値を要約値算出手段11によって算出するステップを有する。すなわち、比較対象となる検査時に係るコンテンツファイル51の要約値を算出するものである。

【0025】この検査時に係る要約値を算出したならば、比較検証手段を構成するステップにおいて、予め基準要約値記憶部2aに記憶されている当該監視対象となっているデジタルコンテンツのコンテンツファイル51の基準要約値を読み出し、検査時に係る要約値を当該基準要約値と比較し、両者の差異を検証する。このステップにより両者間に差異があった場合には、上記コンテン

ツファイルに係るデジタルコンテンツに何らか原因で変更が生じたことを意味する。

【0026】上記比較検証手段による検証結果は、上記プログラムに組み込まれた出力ステップにより、任意の出力手段を通じて出力される。出力手段は、特に限定されるものではなく、改ざん監視装置1のモニタ3に出力することもできるし、モニタ3と共にプリンタ(図示せず)に出力することもできるし、さらには、モニタ3とプリンタの両者に出力することもできる。また、これらと併用してあるいはこれらと併用せずに、監視対象となっているデジタルコンテンツ(ウェブページ)を提供している送信装置5のハードディスクドライブや半導体メモリ等に対し、任意の通信網を介して出力する構成することもできる。任意の通信網とは、本実施形態の改ざん監視装置1と送信装置5とを結ぶ専用回線であってもよいし、パソコン通信やインターネットを利用して、電子メール形態で出力することもできる。

【0027】ここで上記した制御手段10であるプログラムを記録した記録媒体としては、例えば、フレキシブルディスクなどの磁気ディスク、CD-ROM、DVDなどの光ディスク、MO、MDなどの光磁気ディスク、ICカードなどの半導体カード等が挙げられる。また、改ざん監視装置1と通信網を介して接続された任意のコンピュータ(図示せず)のハードディスクドライブ、半導体メモリ等を記録媒体として使用して、通信網を介してプログラムを提供することもできる。また、単一の記録媒体により提供してもよいし、プログラムを複数の記録媒体に分割して格納して提供することもできる。

【0028】次に、本実施形態の改ざん監視装置1を用いた改ざん監視方法の一例を図2のフロー図に基づき説明する。まず、上記したように、予め、監視対象となるデジタルコンテンツ(例えば、ウェブページ)に係るコンテンツファイル51を、改ざん監視装置1の記憶手段2に、例えば、当該ウェブページを提供している送信装置(ウェブサーバ)5にインターネットを通じてアクセスし、ダウンロードする(S100)。この際のウェブページの内容は何らの書き換え、改ざんが行われてないものとし、このコンテンツファイル51のダウンロード時を基準時とする。

【0029】次に、要約値算出手段11により、当該コンテンツファイルのハッシュ値を算出し(S101)、これを基準要約値として、記憶手段2に形成された基準要約値記憶部2aに記憶させる(S102)。

【0030】なお、監視対象となるデジタルコンテンツは、一つであってもよいが、同一の送信装置5が提供している情報中の複数であってもよい。さらには、異なる者によって管理ないし運営されている複数の送信装置5によって提供されている複数の情報を監視対象とすることももちろん可能である。

【0031】基準要約値記憶部2aに記憶されている基

準要約値は、ハッシュ関数による圧縮を行う前の生のコンテンツファイル51と対応させて記憶させておくこともできるが、監視対象が複数存在する場合、改ざん監視装置1の負荷を軽減するため、当該デジタルコンテンツの所在情報、例えば、ウェブページであれば、URLと対応させて格納しておくことが好ましい。従って、図3に示したように、本実施形態では、記憶手段2に、監視対象となっている各デジタルコンテンツ(ウェブページ)のURL記憶部2bが格納されており、各URLに対応させて基準要約値を格納している。

【0032】次に、任意のタイミングで、監視対象に係るデジタルコンテンツ(ウェブページ)を再びダウンロードする(S103)。そして、上記と同様に要約値算出手段11によりハッシュ値を算出する(S104)。このハッシュ値は検査時に係る要約値となる。なお、検査時は、監視対象となっているデジタルコンテンツが複数存在する場合、同じタイミングで設定することもできるし、デジタルコンテンツごとに異なるタイミングを設定することもできる。

【0033】次に、検査時に係る要約値を算出したデジタルコンテンツ(ウェブページ)に対応する基準要約値を、URL記憶部2bに記憶されたURLに基づき、基準要約値記憶部2aから読み出す(S105)。そして、検査時に係る要約値とこの基準要約値とを比較検証し、この検証結果を上記した出力手段により出力する(S106~S108)。

【0034】検証した結果、両者に差異がない場合には、再び、任意の検査タイミングで上記工程を繰り返す。一方、検査結果に差異がある場合には、例えば、改ざん監視装置1のモニタ3やプリンタに検証結果を出力したならば、改ざん監視装置1の管理者ないしは運営者が、その旨を上記デジタルコンテンツ(ウェブページ)を提供している送信装置5の管理者ないしは運営者(情報提供者)に連絡する(S109)。連絡手段としては、電話、ファクシミリ、電子メール等が挙げられるがこれに限定されるものではない。連絡を受けた送信装置5の管理者等は、その差異が、適正な更新作業に基づくものか、不正アクセスによる改ざんに基づくものかを検証する(S110)。その結果、不正アクセスによる改ざんに基づくものである場合には、デジタルコンテンツ(ウェブページ)の送信を停止するなどして、所定の対策をとる(S111)。このように、本実施形態によれば、改ざん監視装置1により、デジタルコンテンツ(ウェブページ)の内容が定期的、あるいは適宜のタイミングで監視されているため、第三者による不正な改ざんを早期に発見し、被害規模の拡大を防ぐことができる。

【0035】一方、上記の検査結果の差異が、適正な更新作業に基づくものである場合には、送信装置5の管理者等は、電話、ファクシミリ、電子メールなどを通じて、改ざん監視装置1の管理者等に連絡する(S11

2)。改ざん監視装置1の管理者等は、この連絡を受けたならば、改めて、ウエブページにアクセスし、新たに基準となるコンテンツファイル51をダウンロードし、ハッシュ値を算出して、当該ウエブページのURLに対応する基準要約値を更新する。なお、この場合、改ざん監視装置1において、例えば電子メールにより適正な更新作業に基づくものである旨の通知を受信したならば、上記ウエブページへのアクセス及び新たに基準となるコンテンツファイル51のダウンロードを自動的に行うように制御手段10をプログラミングしておくこともできる。

【0036】また、検証結果に差異が生じた場合、改ざん監視装置1の管理者等による人の連絡作業を介在せずに、ファクシミリやメールクライアント等を自動起動し、その結果を監視対象となっているデジタルコンテンツ（ウエブページ）を提供している送信装置5に対し、自動的に送信されるように制御手段10をプログラミングし、当該送信装置5のハードディスクドライブ等に直接出力することもできる。

【0037】また、図4に示したように、比較検証の結果、要約値に差異があった場合には、送信装置5に通知する際に（S109）、送信装置5の管理者等が改ざんを確認するに当たってアクセスすべきURLを付加（S109a）して送ることが好ましい。これにより、送信装置5の管理者等における確認作業が容易となる。

【0038】この場合、付加するURLとしては、監視対象となっているウエブページ（デジタルコンテンツ）のURLと、本実施形態の改ざん監視装置1にアクセスするためのURLが考えられるが、前者の場合には、送信装置5の管理者等は、確認後、その旨を改ざん監視装置1へ別途通知（S112）する必要がある。一方、後者の場合には、例えば、図5に示したように、改ざん監視装置1にアクセスすると、内容変更が行われたウエブページ（デジタルコンテンツ）の内容（又はリンク用のURL）と共に、「改ざんされているか否か（不正か適正か）」を判断して入力できるメニューを予め用意しておくことにより、「適正」のボタンを押すだけで、上記実施形態における「改ざん監視装置1への通知（S112）」工程を容易かつ自動的に行うことができる。

【0039】また、図6に示したように、基準要約値の算出ステップ（S101）を経たならば、基準要約値に対して、必要に応じてタイムスタンプを付加した後、改ざん監視装置1が有している秘密鍵を用いて電子署名を作成することもできる（S101a）。そして、基準要約値を基準要約値記憶部2aに記憶せると共に、この電子署名に係る暗号文も記憶手段2に形成した電子署名記憶部2cに記憶させる（S102'）。従って、記憶手段2においてファイル又はテーブルの形式で設定される各記憶部2a, 2b, 2cの構成は、例えば、図7に示したようになる。

【0040】このようにして電子署名も作成した場合には、比較検証ステップ（S106）においては、まず、改ざん監視装置1の公開鍵により、電子署名を復号化し（S106a）、その復号文から得られる基準要約値を基準要約値記憶部2aの基準要約値と比較する（S106b）。両者が一致していれば、基準要約値と検査時に係る要約値とを比較検証する（S106c）。電子署名を作成していない場合には、改ざん監視装置1自体へ不正アクセスした第三者が要約値を書き換えたとしてもその事実を発見することが困難であるが、このように電子署名を作成しておくことにより、基準要約値の書き換え等が行われた否かも検出することができる。従って、比較検証ステップ（S106）において用いる基準要約値は信頼性のあるものとなる。

【0041】なお、上記した電子署名の作成に当たっては、基準要約値に対してそのまま電子署名していたが、さらに、第三者による不正な書き換え等の防止効果を高めるため、基準要約値のダイジェスト（例えば、ハッシュ関数を用いたハッシュ値）を作成し、そのダイジェストに対して、必要に応じてタイムスタンプを付加し、秘密鍵により電子署名することもできる。

【0042】さらに、改ざん監視装置1自体への第三者の不正アクセスを確実に発見する手段として、基準要約値及び／又は電子署名を、基準要約値の算出時及び／又は基準要約値記憶部2aへの基準要約値の記録時、電子署名を作成した場合には電子署名の作成時及び／又は電子署名記憶部2cへの記録時と共に、別途履歴管理しておくことが好ましい。これにより、不正アクセスが介在した場合には、その事実をより確実かつ容易に発見できる。

【0043】この場合、基準要約値及び／又は電子署名に関する上記の各算出時及び／又は記録時の時刻を保証するため、それらのデータに電子署名を行って管理するタイムスタンプサーバ（図示せず）を利用して管理する。タイムスタンプサーバによる電子署名は、改ざん監視装置とは別途のタイムスタンプサーバ独自の秘密鍵を用いて電子署名するため、安全性が高まる。また、タイムスタンプサーバは、改ざん監視装置1と同一のコンピュータ内に設定することも可能であるが、別のコンピュータに設定しておくことが安全性の点から好ましい。

【0044】

【発明の効果】本発明のデジタルコンテンツの改ざん監視装置、改ざん監視方法及び記録媒体によれば、デジタルコンテンツを任意のタイミングで検査し監視しているため、内容が変更された事実を早期に発見できる。従って、比較検証結果を出力して監視対象となっているデジタルコンテンツの情報提供者に知らせることで、不正な改ざんによるものか否かの注意を喚起でき、被害規模の拡大を防ぐことができる。また、一方向関数による要約

値を用いて監視しているため、比較検証を迅速に行うことができる。特に、ハッシュ関数を用いた場合には、監視対象のデジタルコンテンツの内容が少しでも異なれば結果として得られるハッシュ値が大きく変わるために、比較検証を確実に行うことができる。

【図面の簡単な説明】

【図1】図1は、本発明の一の実施形態にかかる改ざん監視装置を示す構成図である。

【図2】図2は、本発明の一の実施形態にかかる改ざん監視方法を説明するためのフロー図である。

【図3】図3は、上記実施形態にかかる改ざん監視装置の記憶手段に形成される基準要約値記憶部及びURL記憶部の概略構成を示す図である。

【図4】図4は、他の態様に係る改ざん監視方法において、上記実施形態の改ざん監視方法と相違する点を示したフロー図である。

【図5】図5は、図4のS109aにおいて付加したURLにアクセスして表示された状態の一例を示す図である。

る。

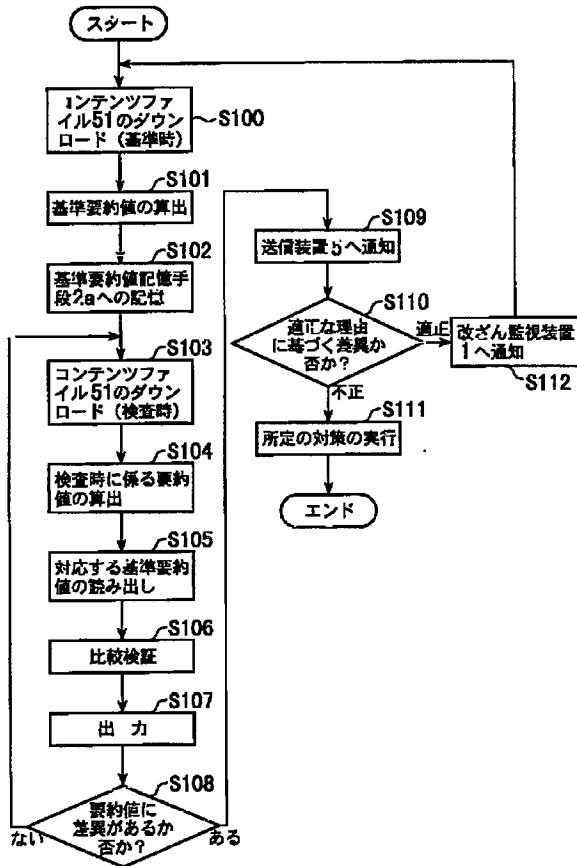
【図6】図6は、さらに他の態様に係る改ざん監視方法において、上記実施形態の改ざん監視方法と相違する点を示したフロー図である。

【図7】図7は、上記他の態様に係る改ざん監視装置の記憶手段に形成される基準要約値記憶部、URL記憶部及び電子署名記憶部の概略構成を示す図である

【符号の説明】

- 1 改ざん監視装置
- 2 記憶手段
- 10 制御手段
- 11 要約値算出手段
- 2a 基準要約値記憶部
- 2b URL記憶部
- 2c 電子署名記憶部
- 5 送信装置
- 51 コンテンツファイル
- 51-1 テキスト、画像などのデジタルコンテンツ
- 51-2 インターネット
- 51-3 モニタ
- 51-4 入出力制御部
- 51-5 モニタ
- 51-6 URL
- 51-7 モニタ
- 51-8 URL
- 51-9 モニタ
- 51-10 URL
- 51-11 URL
- 51-12 URL
- 51-13 URL
- 51-14 URL
- 51-15 URL
- 51-16 URL
- 51-17 URL
- 51-18 URL
- 51-19 URL
- 51-20 URL
- 51-21 URL
- 51-22 URL
- 51-23 URL
- 51-24 URL
- 51-25 URL
- 51-26 URL
- 51-27 URL
- 51-28 URL
- 51-29 URL
- 51-30 URL
- 51-31 URL
- 51-32 URL
- 51-33 URL
- 51-34 URL
- 51-35 URL
- 51-36 URL
- 51-37 URL
- 51-38 URL
- 51-39 URL
- 51-40 URL
- 51-41 URL
- 51-42 URL
- 51-43 URL
- 51-44 URL
- 51-45 URL
- 51-46 URL
- 51-47 URL
- 51-48 URL
- 51-49 URL
- 51-50 URL
- 51-51 URL
- 51-52 URL
- 51-53 URL
- 51-54 URL
- 51-55 URL
- 51-56 URL
- 51-57 URL
- 51-58 URL
- 51-59 URL
- 51-60 URL
- 51-61 URL
- 51-62 URL
- 51-63 URL
- 51-64 URL
- 51-65 URL
- 51-66 URL
- 51-67 URL
- 51-68 URL
- 51-69 URL
- 51-70 URL
- 51-71 URL
- 51-72 URL
- 51-73 URL
- 51-74 URL
- 51-75 URL
- 51-76 URL
- 51-77 URL
- 51-78 URL
- 51-79 URL
- 51-80 URL
- 51-81 URL
- 51-82 URL
- 51-83 URL
- 51-84 URL
- 51-85 URL
- 51-86 URL
- 51-87 URL
- 51-88 URL
- 51-89 URL
- 51-90 URL
- 51-91 URL
- 51-92 URL
- 51-93 URL
- 51-94 URL
- 51-95 URL
- 51-96 URL
- 51-97 URL
- 51-98 URL
- 51-99 URL
- 51-100 URL
- 51-101 URL
- 51-102 URL
- 51-103 URL
- 51-104 URL
- 51-105 URL
- 51-106 URL
- 51-107 URL
- 51-108 URL
- 51-109 URL
- 51-110 URL
- 51-111 URL
- 51-112 URL
- 51-113 URL
- 51-114 URL
- 51-115 URL
- 51-116 URL
- 51-117 URL
- 51-118 URL
- 51-119 URL
- 51-120 URL
- 51-121 URL
- 51-122 URL
- 51-123 URL
- 51-124 URL
- 51-125 URL
- 51-126 URL
- 51-127 URL
- 51-128 URL
- 51-129 URL
- 51-130 URL
- 51-131 URL
- 51-132 URL
- 51-133 URL
- 51-134 URL
- 51-135 URL
- 51-136 URL
- 51-137 URL
- 51-138 URL
- 51-139 URL
- 51-140 URL
- 51-141 URL
- 51-142 URL
- 51-143 URL
- 51-144 URL
- 51-145 URL
- 51-146 URL
- 51-147 URL
- 51-148 URL
- 51-149 URL
- 51-150 URL
- 51-151 URL
- 51-152 URL
- 51-153 URL
- 51-154 URL
- 51-155 URL
- 51-156 URL
- 51-157 URL
- 51-158 URL
- 51-159 URL
- 51-160 URL
- 51-161 URL
- 51-162 URL
- 51-163 URL
- 51-164 URL
- 51-165 URL
- 51-166 URL
- 51-167 URL
- 51-168 URL
- 51-169 URL
- 51-170 URL
- 51-171 URL
- 51-172 URL
- 51-173 URL
- 51-174 URL
- 51-175 URL
- 51-176 URL
- 51-177 URL
- 51-178 URL
- 51-179 URL
- 51-180 URL
- 51-181 URL
- 51-182 URL
- 51-183 URL
- 51-184 URL
- 51-185 URL
- 51-186 URL
- 51-187 URL
- 51-188 URL
- 51-189 URL
- 51-190 URL
- 51-191 URL
- 51-192 URL
- 51-193 URL
- 51-194 URL
- 51-195 URL
- 51-196 URL
- 51-197 URL
- 51-198 URL
- 51-199 URL
- 51-200 URL
- 51-201 URL
- 51-202 URL
- 51-203 URL
- 51-204 URL
- 51-205 URL
- 51-206 URL
- 51-207 URL
- 51-208 URL
- 51-209 URL
- 51-210 URL
- 51-211 URL
- 51-212 URL
- 51-213 URL
- 51-214 URL
- 51-215 URL
- 51-216 URL
- 51-217 URL
- 51-218 URL
- 51-219 URL
- 51-220 URL
- 51-221 URL
- 51-222 URL
- 51-223 URL
- 51-224 URL
- 51-225 URL
- 51-226 URL
- 51-227 URL
- 51-228 URL
- 51-229 URL
- 51-230 URL
- 51-231 URL
- 51-232 URL
- 51-233 URL
- 51-234 URL
- 51-235 URL
- 51-236 URL
- 51-237 URL
- 51-238 URL
- 51-239 URL
- 51-240 URL
- 51-241 URL
- 51-242 URL
- 51-243 URL
- 51-244 URL
- 51-245 URL
- 51-246 URL
- 51-247 URL
- 51-248 URL
- 51-249 URL
- 51-250 URL
- 51-251 URL
- 51-252 URL
- 51-253 URL
- 51-254 URL
- 51-255 URL
- 51-256 URL
- 51-257 URL
- 51-258 URL
- 51-259 URL
- 51-260 URL
- 51-261 URL
- 51-262 URL
- 51-263 URL
- 51-264 URL
- 51-265 URL
- 51-266 URL
- 51-267 URL
- 51-268 URL
- 51-269 URL
- 51-270 URL
- 51-271 URL
- 51-272 URL
- 51-273 URL
- 51-274 URL
- 51-275 URL
- 51-276 URL
- 51-277 URL
- 51-278 URL
- 51-279 URL
- 51-280 URL
- 51-281 URL
- 51-282 URL
- 51-283 URL
- 51-284 URL
- 51-285 URL
- 51-286 URL
- 51-287 URL
- 51-288 URL
- 51-289 URL
- 51-290 URL
- 51-291 URL
- 51-292 URL
- 51-293 URL
- 51-294 URL
- 51-295 URL
- 51-296 URL
- 51-297 URL
- 51-298 URL
- 51-299 URL
- 51-300 URL
- 51-301 URL
- 51-302 URL
- 51-303 URL
- 51-304 URL
- 51-305 URL
- 51-306 URL
- 51-307 URL
- 51-308 URL
- 51-309 URL
- 51-310 URL
- 51-311 URL
- 51-312 URL
- 51-313 URL
- 51-314 URL
- 51-315 URL
- 51-316 URL
- 51-317 URL
- 51-318 URL
- 51-319 URL
- 51-320 URL
- 51-321 URL
- 51-322 URL
- 51-323 URL
- 51-324 URL
- 51-325 URL
- 51-326 URL
- 51-327 URL
- 51-328 URL
- 51-329 URL
- 51-330 URL
- 51-331 URL
- 51-332 URL
- 51-333 URL
- 51-334 URL
- 51-335 URL
- 51-336 URL
- 51-337 URL
- 51-338 URL
- 51-339 URL
- 51-340 URL
- 51-341 URL
- 51-342 URL
- 51-343 URL
- 51-344 URL
- 51-345 URL
- 51-346 URL
- 51-347 URL
- 51-348 URL
- 51-349 URL
- 51-350 URL
- 51-351 URL
- 51-352 URL
- 51-353 URL
- 51-354 URL
- 51-355 URL
- 51-356 URL
- 51-357 URL
- 51-358 URL
- 51-359 URL
- 51-360 URL
- 51-361 URL
- 51-362 URL
- 51-363 URL
- 51-364 URL
- 51-365 URL
- 51-366 URL
- 51-367 URL
- 51-368 URL
- 51-369 URL
- 51-370 URL
- 51-371 URL
- 51-372 URL
- 51-373 URL
- 51-374 URL
- 51-375 URL
- 51-376 URL
- 51-377 URL
- 51-378 URL
- 51-379 URL
- 51-380 URL
- 51-381 URL
- 51-382 URL
- 51-383 URL
- 51-384 URL
- 51-385 URL
- 51-386 URL
- 51-387 URL
- 51-388 URL
- 51-389 URL
- 51-390 URL
- 51-391 URL
- 51-392 URL
- 51-393 URL
- 51-394 URL
- 51-395 URL
- 51-396 URL
- 51-397 URL
- 51-398 URL
- 51-399 URL
- 51-400 URL
- 51-401 URL
- 51-402 URL
- 51-403 URL
- 51-404 URL
- 51-405 URL
- 51-406 URL
- 51-407 URL
- 51-408 URL
- 51-409 URL
- 51-410 URL
- 51-411 URL
- 51-412 URL
- 51-413 URL
- 51-414 URL
- 51-415 URL
- 51-416 URL
- 51-417 URL
- 51-418 URL
- 51-419 URL
- 51-420 URL
- 51-421 URL
- 51-422 URL
- 51-423 URL
- 51-424 URL
- 51-425 URL
- 51-426 URL
- 51-427 URL
- 51-428 URL
- 51-429 URL
- 51-430 URL
- 51-431 URL
- 51-432 URL
- 51-433 URL
- 51-434 URL
- 51-435 URL
- 51-436 URL
- 51-437 URL
- 51-438 URL
- 51-439 URL
- 51-440 URL
- 51-441 URL
- 51-442 URL
- 51-443 URL
- 51-444 URL
- 51-445 URL
- 51-446 URL
- 51-447 URL
- 51-448 URL
- 51-449 URL
- 51-450 URL
- 51-451 URL
- 51-452 URL
- 51-453 URL
- 51-454 URL
- 51-455 URL
- 51-456 URL
- 51-457 URL
- 51-458 URL
- 51-459 URL
- 51-460 URL
- 51-461 URL
- 51-462 URL
- 51-463 URL
- 51-464 URL
- 51-465 URL
- 51-466 URL
- 51-467 URL
- 51-468 URL
- 51-469 URL
- 51-470 URL
- 51-471 URL
- 51-472 URL
- 51-473 URL
- 51-474 URL
- 51-475 URL
- 51-476 URL
- 51-477 URL
- 51-478 URL
- 51-479 URL
- 51-480 URL
- 51-481 URL
- 51-482 URL
- 51-483 URL
- 51-484 URL
- 51-485 URL
- 51-486 URL
- 51-487 URL
- 51-488 URL
- 51-489 URL
- 51-490 URL
- 51-491 URL
- 51-492 URL
- 51-493 URL
- 51-494 URL
- 51-495 URL
- 51-496 URL
- 51-497 URL
- 51-498 URL
- 51-499 URL
- 51-500 URL
- 51-501 URL
- 51-502 URL
- 51-503 URL
- 51-504 URL
- 51-505 URL
- 51-506 URL
- 51-507 URL
- 51-508 URL
- 51-509 URL
- 51-510 URL
- 51-511 URL
- 51-512 URL
- 51-513 URL
- 51-514 URL
- 51-515 URL
- 51-516 URL
- 51-517 URL
- 51-518 URL
- 51-519 URL
- 51-520 URL
- 51-521 URL
- 51-522 URL
- 51-523 URL
- 51-524 URL
- 51-525 URL
- 51-526 URL
- 51-527 URL
- 51-528 URL
- 51-529 URL
- 51-530 URL
- 51-531 URL
- 51-532 URL
- 51-533 URL
- 51-534 URL
- 51-535 URL
- 51-536 URL
- 51-537 URL
- 51-538 URL
- 51-539 URL
- 51-540 URL
- 51-541 URL
- 51-542 URL
- 51-543 URL
- 51-544 URL
- 51-545 URL
- 51-546 URL
- 51-547 URL
- 51-548 URL
- 51-549 URL
- 51-550 URL
- 51-551 URL
- 51-552 URL
- 51-553 URL
- 51-554 URL
- 51-555 URL
- 51-556 URL
- 51-557 URL
- 51-558 URL
- 51-559 URL
- 51-560 URL
- 51-561 URL
- 51-562 URL
- 51-563 URL
- 51-564 URL
- 51-565 URL
- 51-566 URL
- 51-567 URL
- 51-568 URL
- 51-569 URL
- 51-570 URL
- 51-571 URL
- 51-572 URL
- 51-573 URL
- 51-574 URL
- 51-575 URL
- 51-576 URL
- 51-577 URL
- 51-578 URL
- 51-579 URL
- 51-580 URL
- 51-581 URL
- 51-582 URL
- 51-583 URL
- 51-584 URL
- 51-585 URL
- 51-586 URL
- 51-587 URL
- 51-588 URL
- 51-589 URL
- 51-590 URL
- 51-591 URL
- 51-592 URL
- 51-593 URL
- 51-594 URL
- 51-595 URL
- 51-596 URL
- 51-597 URL
- 51-598 URL
- 51-599 URL
- 51-600 URL
- 51-601 URL
- 51-602 URL
- 51-603 URL
- 51-604 URL
- 51-605 URL
- 51-606 URL
- 51-607 URL
- 51-608 URL
- 51-609 URL
- 51-610 URL
- 51-611 URL
- 51-612 URL
- 51-613 URL
- 51-614 URL
- 51-615 URL
- 51-616 URL
- 51-617 URL
- 51-618 URL
- 51-619 URL
- 51-620 URL
- 51-621 URL
- 51-622 URL
- 51-623 URL
- 51-624 URL
- 51-625 URL
- 51-626 URL
- 51-627 URL
- 51-628 URL
- 51-629 URL
- 51-630 URL
- 51-631 URL
- 51-632 URL
- 51-633 URL
- 51-634 URL
- 51-635 URL
- 51-636 URL
- 51-637 URL
- 51-638 URL
- 51-639 URL
- 51-640 URL
- 51-641 URL
- 51-642 URL
- 51-643 URL
- 51-644 URL
- 51-645 URL
- 51-646 URL
- 51-647 URL
- 51-648 URL
- 51-649 URL
- 51-650 URL
- 51-651 URL
- 51-652 URL
- 51-653 URL
- 51-654 URL
- 51-655 URL
- 51-656 URL
- 51-657 URL
- 51-658 URL
- 51-659 URL
- 51-660 URL
- 51-661 URL
- 51-662 URL
- 51-663 URL
- 51-664 URL
- 51-665 URL
- 51-666 URL
- 51-667 URL
- 51-668 URL
- 51-669 URL
- 51-670 URL
- 51-671 URL
- 51-672 URL
- 51-673 URL
- 51-674 URL
- 51-675 URL
- 51-676 URL
- 51-677 URL
- 51-678 URL
- 51-679 URL
- 51-680 URL
- 51-681 URL
- 51-682 URL
- 51-683 URL
- 51-684 URL
- 51-685 URL
- 51-686 URL
- 51-687 URL
- 51-688 URL
- 51-689 URL
- 51-690 URL
- 51-691 URL
- 51-692 URL
- 51-693 URL
- 51-694 URL
- 51-695 URL
- 51-696 URL
- 51-697 URL
- 51-698 URL
- 51-699 URL
- 51-700 URL
- 51-701 URL
- 51-702 URL
- 51-703 URL
- 51-704 URL
- 51-705 URL
- 51-706 URL
- 51-707 URL
- 51-708 URL
- 51-709 URL
- 51-710 URL
- 51-711 URL
- 51-712 URL
- 51-713 URL
- 51-714 URL
- 51-715 URL
- 51-716 URL
- 51-717 URL
- 51-718 URL
- 51-719 URL
- 51-720 URL
- 51-721 URL
- 51-722 URL
- 51-723 URL
- 51-724 URL
- 51-725 URL
- 51-726 URL
- 51-727 URL
- 51-728 URL
- 51-729 URL
- 51-730 URL
- 51-731 URL
- 51-732 URL
- 51-733 URL
- 51-734 URL
- 51-735 URL
- 51-736 URL
- 51-737 URL
- 51-738 URL
- 51-739 URL
- 51-740 URL
- 51-741 URL
- 51-742 URL
- 51-743 URL
- 51-744 URL
- 51-745 URL
- 51-746 URL
- 51-747 URL
- 51-748 URL
- 51-749 URL
- 51-750 URL
- 51-751 URL
- 51-752 URL
- 51-753 URL
- 51-754 URL
- 51-755 URL
- 51-756 URL
- 51-757 URL
- 51-758 URL
- 51-759 URL
- 51-760 URL
- 51-761 URL
- 51-762 URL
- 51-763 URL
- 51-764 URL
- 51-765 URL
- 51-766 URL
- 51-767 URL
- 51-768 URL
- 51-769 URL
- 51-770 URL
- 51-771 URL
- 51-772 URL
- 51-773 URL
- 51-774 URL
- 51-775 URL
- 51-776 URL
- 51-777 URL
- 51-778 URL
- 51-779 URL
- 51-780 URL
- 51-781 URL
- 51-782 URL
- 51-783 URL
- 51-784 URL
- 51-785 URL
- 51-786 URL
- 51-787 URL
- 51-788 URL
- 51-789 URL
- 51-790 URL
- 51-791 URL
- 51-792 URL
- 51-793 URL
- 51-794 URL
- 51-795 URL
- 51-796 URL
- 51-797 URL
- 51-798 URL
- 51-799 URL
- 51-800 URL
- 51-801 URL
- 51-802 URL
- 51-803 URL
- 51-804 URL
- 51-805 URL
- 51-806 URL
- 51-807 URL
- 51-808 URL
- 51-809 URL
- 51-810 URL
- 51-811 URL
- 51-812 URL
- 51-813 URL
- 51-814 URL
- 51-815 URL
- 51-816 URL
- 51-817 URL
- 51-818 URL
- 51-819 URL
- 51-820 URL
- 51-821 URL
- 51-822 URL
- 51-823 URL
- 51-824 URL
- 51-825 URL
- 51-826 URL
- 51-827 URL
- 51-828 URL
- 51-829 URL
- 51-830 URL
- 51-831 URL
- 51-832 URL
- 51-833 URL
- 51-834 URL
- 51-835 URL
- 51-836 URL
- 51-837 URL
- 51-838 URL
- 51-839 URL
- 51-840 URL
- 51-841 URL
- 51-842 URL
- 51-843 URL
- 51-844 URL
- 51-845 URL
- 51-846 URL
- 51-847 URL
- 51-848 URL
- 51-849 URL
- 51-850 URL
- 51-851 URL
- 51-852 URL
- 51-853 URL
- 51-854 URL
- 51-855 URL
- 51-856 URL
- 51-857 URL
- 51-858 URL
- 51-859 URL
- 51-860 URL
- 51-861 URL
- 51-862 URL
- 51-863 URL
- 51-864 URL
- 51-865 URL
- 51-866 URL
- 51-867 URL
- 51-868 URL
- 51-869 URL
- 51-870 URL
- 51-871

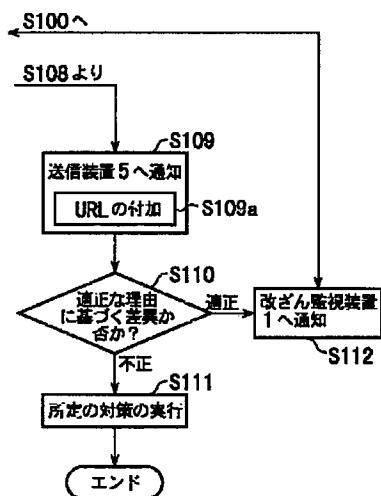
【図2】



【図3】

2b	2a
URI.記憶部 No. 1. http://www~/ No. 2. http://www~/ No. n. http://www~/	基準要約値記憶部 (ハッシュ用) No. 1. 158DA43F0-- No. 2. 29348ADC5-- No. n. 15289DA85--

【図4】



【図5】



【図7】

2b	2a	2c
URL記憶部	基準要約値記憶部 (ハッシュ値)	電子署名記憶部
No. 1. http://www~/ No. 2. http://www~/	No. 1. 158DA43FO -- No. 2. 29348ADC5 --	No. 1. 63296XB5 --- No. 2. 0891V/C ---
No. n. http://www~/	No. n. 15289DA85 --	No. n. 337EG632. ---

フロントページの続き

(72)発明者 杉江 修

愛知県名古屋市中村区名駅南一丁目27番2
号 株式会社シーティーアイ内

F ターム(参考) 5B017 AA08 BA09 BB02 CA16
5J104 AA08 AA09 LA01 LA05 LA06
NA11 NA12 NA27 PA07 PA09
9A001 BB02 BB03 BB04 CC02 DD09
EE02 EE03 GG21 JJ13 JJ25
JJ27 JJ67 JZ14 KK42 KK43
KK60 LL03